UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/700,622 | 11/05/2003 | Takashi Kokubo | 04329.3173 | 5368 |

22852 7590 06/23/2008
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

| EXAMINER | |
|---|---|
| RAHIM, MONJUR | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2134 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/23/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|  |  |  |  |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/700,622 | **Applicant(s)**<br>KOKUBO ET AL. | |
| | **Examiner**<br>MONJOUR RAHIM | **Art Unit**<br>2134 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *05 November 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 November 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *11/5/2003, 4/13/2004, 10/28/2004, 6/29/2005*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

### *DETAILED ACTION*

1. ***Claims 1-20*** pending.

2. ***Claims 1-20*** rejected.

### ***Information Disclosure Statement***

3. The Information Disclosure Statement (IDS) submitted on 11/05/2003 compliance with the provisions of 37 CFR 1.97. Accordingly, the IDS statement is being considered by the examiner.

### ***Priority***

4. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 2002-321355 (Japan), filed on 11/05/2002.

### ***Drawings***

5. The drawings filed on 11/05/2003 are accepted by the examiner.

### ***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

***Claims 1-20*** are rejected under 35 U.S.C. 102(b) as being anticipated Staring et al. (US PG-Pub No. 2001/0007127 A1) hereinafter Staring.

As per ***claim 1***, Staring discloses:

**- a padding unit which adds data to an asynchronous packet to form an integer multiple of a block length** (Staring, paragraph [0049], "One alternative is to add padding bytes so that the block-length equals eight again. However, this increases the data payload size and in addition, the number of padded bytes must be conveyed to the decrypting side to remove the padding bytes correctly. A better method is to use Cipher Text Stealing. All 8-byte blocks are encrypted sequentially except for the last 8-byte block and the remaining bytes in the last `incomplete` data block"), where padding was added data and , where data is a  is a asynchronous/synchronous, as claimed and (Staring, paragraph [0038], "Once the session has actually started, the data field is normally mainly used for carrying parts of the information to be transferred (using either asynchronous or isochronous packets, depending on the application and communication system);

**- an encryption unit which encrypts the asynchronous packet added by the padding unit and a synchronous packet** (Staring, paragraph [0039], "If a block cipher in CBC mode is used to encrypt the data of the packet, it is preferred that the key check block has the same length as (or a multiple of) the block size of the encryption algorithm"), where inherently encryption done by a system/software/unit, as claimed;

**- a transmitting unit which transmits the added asynchronous packet and the synchronous packet encrypted by the encryption unit** (Staring, paragraph [0052], "The sender retains the last clear-text eight bytes from the previous packet, called the key check block, and encrypts this block with the current session key. The Host may have decided to change the session key between the previous packet and the current packet. In this case, the key check block gets encrypted with a different session key than the one used to encrypt the last eight bytes from the previous packet"), where packet encrypted inherently by the encryptor/software, which can be called units, as claimed.

As per ***claim 2***, claim 1 is incorporated and Staring discloses:

**- a data length information adder which adds data length information on the length of the real data of the asynchronous packet to the encrypted added asynchronous packet** (Staring, paragraph [0049], "A better method is to use Cipher Text Stealing. All 8-byte blocks are encrypted sequentially except for the last 8-byte block and the remaining bytes in the last `incomplete` data block. These bytes are concatenated into one extended block and treated separately. The extended block-length thus ranges between 9 and 15 bytes").

As per ***claim 3***, claim 1 is incorporated and Staring discloses:

**- a key management unit which rewrites the key information used for encryption by the encryption unit, based on key rewrite information, and adds the key rewrite information to the encrypted added asynchronous packet** (Staring, paragraph [0039], "For instance, a random number generator may be used fed by initial key information exchanged between the source and sink device. A key changer 114 triggers the key generator 112 to generate a source session key for use as the active source session key for at least one packet to be encrypted next. The algorithm controlling the key change can be very simple, e.g. every successive packet may be encrypted using a next session key, or at regular times like every second (e.g. controlled by a timer) a next session key may be used. An encryptor 116 is used to encrypt at least part of the data field of a packet under control of the active source session key").

As per ***claim 4***, claim 1 is incorporated and Staring discloses:

**- a copy control information adder which adds copy control information which limits the number of times  the asynchronous packet is copied, to the encrypted added asynchronous packet** (Staring, paragraph [0021], "As defined in the measure of the dependent claim 8, the key check block is a direct `copy` of part of the data in a preceding packet. .... Preferably, the data block containing the (encrypted) data for the next key check block is located in the second or last block of the encrypted part of the data field"), where "copy" task inherently logged by the system/software.

As per ***claim 5***, claim 1 is incorporated and Staring discloses:

**- an adder which inserts, between the encrypted added asynchronous packets, selected one of control information including data length information on a length of real data of the asynchronous packet, key rewrite information which rewrites key information used for encryption by the encryption unit and copy control information for limiting the number of times the asynchronous packet is copied** (Staring, paragraph [0049], "The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again….. Finally, block 3 is encrypted. Note that part of block 3 was already encrypted in the previous stage and is encrypted again in the last stage").

As per ***claim 6***, claim 1 is incorporated and Staring discloses:

**- a receiving unit which receives the encrypted added asynchronous packet transmitted from the transmitting unit** (Staring, paragraph [0037], "The devices include conventional means to transmit and receive packets via the medium 150. Depending on the medium, such means may be formed by a telephone or cable modem, or a bus interface"), where medium 150 is the receiving unit, as claimed;

**- a decryption unit which decrypts the encrypted added asynchronous packet received by the receiving unit and outputs the added asynchronous packet** (Staring, paragraph [ 0027], "determining which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by decrypting the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found");

**- an extraction unit which extracts real data, except for the data added by the padding unit, from the added asynchronous packet output from the decryption unit** (Staring, paragraph [0005], "is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method"), where "decrypted data, which make sense" is the real data, as claimed.

As per ***claim 7,*** claim 6 is incorporated and Staring discloses:

**- wherein the extraction unit detects data length information on a length of the real data of the asynchronous packet and based on the detected data length**

**information, extracts the real data except for the added data, from the added asynchronous packet output from the decryption unit** (Staring, paragraph [0013], "a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key"), where "part of the data field" is the length parameter, as claimed.

As per ***claim 8,*** claim 6 is incorporated and Staring discloses:

**- wherein the decryption unit detects key rewrite information which rewrites key information used for encryption by the encryption unit and, based on the latest key information rewritten by the key rewrite information, decrypts the encrypted added asynchronous packet received by the receiving unit** (Staring, paragraph [0013], "a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key"), where "part of the data field" is the length parameter, as claimed.

As per ***claim 9,*** claim 6 is incorporated and Staring discloses:

**- a copy function which detects copy control information for limiting the number of times the asynchronous packet received by the receiving unit is copied and copies at least the asynchronous packet within the limit** (Staring, paragraph [0049], "The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again..... Finally, block 3 is encrypted. Note that part of block 3 was already encrypted in the previous stage and is encrypted again in the last stage").

As per ***claim 10***, claim 6 is incorporated and Staring discloses:

**- wherein the receiving unit receives selected one of control information including the data length information on a length of the real data of the asynchronous packet, key rewrite information which rewrites key information used for encryption by the encryption unit and copy control information for limiting the**

**number of times the asynchronous packet is copied** (Staring, paragraph [0049], "The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again..... Finally, block 3 is encrypted. Note that part of block 3 was already encrypted in the previous stage and is encrypted again in the last stage").

As per ***claim 11***, Staring discloses:

**- adding data to the asynchronous packet to form an integer multiple of a block length** (Staring, paragraph [0049], "To preserve data payloads and to minimize data payload overhead, Cipher Text Stealing CTS) is preferably used. The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again"), where "padding" is the adding data to the asynchronous packet to make 8-byte block-length, as claimed;

**- encrypting the added asynchronous packet and the synchronous packet** (Staring, paragraph [0041, "This makes it very simple to verify which candidate sink key corresponds to the sink key used for encrypting the received packet. For instance, the first candidate sink key may be used to decrypt the data in the key check block field. If the decrypted data matches the reference key check block, this candidate key is the desired key. If not, the next candidate key can be used until a match has been found"), where data being encrypted, as claimed;

**- and transmitting the encrypted added asynchronous packet and the encrypted synchronous packet** (Staring, paragraph [0054], "This process is repeated until all the data has been transmitted. It is at the sole discretion of the sender to decide when to reenter phase 3 to update the session key").

As per ***claim 12***, claim 11 is incorporated and Staring discloses:

**- adding data length information on the length of the real data of the asynchronous packet to the encrypted added asynchronous packet** (Staring, paragraph [0049], "To preserve data payloads and to minimize data payload overhead, Cipher Text Stealing CTS) is preferably used. The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again"), where "padding" is the adding data to the asynchronous packet to make 8-byte block-length, as claimed.

As per ***claim 13***, claim 11 is incorporated and Staring discloses:

**- rewriting the key information used for encryption based on key rewrite information, and adding the key rewrite information to the encrypted added asynchronous packet** (Staring, paragraph [0039], "For instance, a random number generator may be used fed by initial key information exchanged between the source and sink device. A key changer 114 triggers the key generator 112 to generate a source session key for use as the active source session key for at least one packet to be encrypted next. The algorithm controlling the key change can be very simple, e.g. every successive packet may be encrypted using a next session key, or at regular times like every second (e.g. controlled by a timer) a next session key may be used. An encryptor 116 is used to encrypt at least part of the data field of a packet under control of the active source session key").

As per ***claim 14***, claim 11 is incorporated and Staring discloses:

**- adding copy control information for limiting the number of times the asynchronous packet is copied, to the encrypted added asynchronous packet** (Staring, paragraph [0049], "The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again..... Finally, block 3 is encrypted. Note that part of block 3 was already encrypted in the previous stage and is encrypted again in the last stage").

As per ***claim 15***, claim 11 is incorporated and Staring discloses:

- **inserting, between the encrypted added asynchronous packets, one of the control information including data length information on a length of real data of the asynchronous packet, key rewrite information which rewrites key information used for encryption, and the copy control information for limiting the number of times the asynchronous packet is copied** (Staring, paragraph [0049], "The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again..... Finally, block 3 is encrypted. Note that part of block 3 was already encrypted in the previous stage and is encrypted again in the last stage").

As per ***claim 16***, claim 11 is incorporated and Staring discloses:

- **receiving the encrypted added asynchronous packet transmitted** (Staring, paragraph [0037], "The devices include conventional means to transmit and receive packets via the medium 150");

- **decrypting the encrypted added asynchronous packet and outputs the added asynchronous packet** (Staring, paragraph [0040], "To this end, the key resolver 136 is operative to cause the decryptor 134 to decrypt the data in the key check block field of a received packet under control of a plurality of candidate sink session keys. Preferably after each decryption, the key resolver 136 verifies whether the tested candidate sink session key produced a correct decryption result of the key check block transferred via the key check block field. This is repeated until the key has been found. The candidate key that produced a correct decryption result is then selected for further use");

- **and extracting real data except for the added data from the added asynchronous packet** (Staring, paragraph [(Staring, paragraph [0005], "is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method"), where "decrypted data, which make sense" is the real data, as claimed.

As per ***claim 17***, claim 16 is incorporated and Staring discloses:

**- wherein data length information on a length of the real data of the asynchronous packet is detected and, based on the detected data length information, the real data except for the added data is extracted from the decrypted added asynchronous packet** (Staring, paragraph [(Staring, paragraph [0013], "a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key"), where "part of the data field" is the length parameter, as claimed.

As per ***claim 18***, claim 16 is incorporated and Staring discloses:

**- detecting key rewrite information which rewrites key information used for encryption is detected, and based on the latest key information rewritten by the detected key rewrite information, the encrypted added asynchronous packet received is decrypted** (Staring, paragraph [0049], "The DES algorithm uses an 8-byte block-length to operate on. Therefore, whenever the data payload is not a multiple of eight bytes, some measures must be taken to encrypt the last data block, which contains less than eight bytes. One alternative is to add padding bytes so that the block-length equals eight again..... Finally, block 3 is encrypted. Note that part of block 3 was already encrypted in the previous stage and is encrypted again in the last stage").

As per ***claim 19***, claim 16 is incorporated and Staring discloses:

**- detecting copy control information for limiting the number of times the asynchronous packet is copied, and copying at least the asynchronous packet within**

**the limit** (Staring, paragraph [0021], "As defined in the measure of the dependent claim 8, the key check block is a direct `copy` of part of the data in a preceding packet. .... Preferably, the data block containing the (encrypted) data for the next key check block is located in the second or last block of the encrypted part of the data field"), where "copy" task inherently logged by the system/software.

As per ***claim 20,*** claim 16 is incorporated and Staring discloses:

**- wherein one of the control information including the data length information on a length of the real data of the asynchronous packet, key rewrite information which rewrites key information used for encryption and copy control information for limiting the number of times the asynchronous packet is copied, is received as an exclusive control information packet** (Staring, paragraph [0021], "As defined in the measure of the dependent claim 8, the key check block is a direct `copy` of part of the data in a preceding packet. .... Preferably, the data block containing the (encrypted) data for the next key check block is located in the second or last block of the encrypted part of the data field"), where "copy" task inherently logged by the system/software.

### *Conclusion*

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see form "PTO-892 Notice of Reference Cited").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monjour Rahim whose telephone number is (571)270-3890. The examiner can normally be reached on 5:30 AM -3:30 PM (Mo-Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571)272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (in USA or CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2134
Date: 06/18/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134